CTF-提权

原创

采姑娘の小蘑菇 于 2021-01-06 18:48:38 发布 420 收藏 1

分类专栏： CTF 文章标签： 网络安全

本文链接：https://blog.csdn.net/su__xiaoyan/article/details/112277252

提权

> 通过Web服务拿下服务器的基础权限以后（www-data），如何提权值最高的系统权限（root）。

> **提权的前提条件：**
>
> 1. 获取服务器的基础权限。
> 2. 能上传或者下载文件。
> 3. 靶机上面有常见工具或者环境，例如nc，python或者Perl。

> **Linux操作系统提权方法：**
>
> 1. 利用内核漏洞进行提权
> 2. 利用错误的系统配置进行提权
> 3. 明文密码提权
> 4. 计划任务提权
> 5. 密码复用提权

> **内核漏洞提权**
>
> 1. 首先查看系统Linux的发行版本：
>   cat /etc/issue
>   cat /etc/*-release
> 2. 查看内核版本
>   uname -a
> 3. 查看是否具有内核溢出漏洞
>   searchsploit Linux发行版本/内核版本
> 4. 如果存在内核溢出漏洞的话，可以上传内核溢出代码，编译执行。
>   gcc xxx -o yyy （有些溢出代码在编译的时候需要特定参数）
>   chmod +x yyy
>   ./yyy

明文密码提权

1. 获取/etc/passwd和/etc/shadow
   默认情况下/etc/passwd全用户可读，root用户可写；/etc/shadow仅root用户可读可写。
2. 通过/etc/passwd和/etc/shadow合成一个可以破解版的文件
   命令：unshadow passwd shadow > new_shadow
3. 开始破解，获得明文密码
   john new_shadow

计划任务提权

- 系统中的一些定时执行的任务，一般由crontab来管理，具有所属用户的权限，非root权限的用户不能列出。但是/etc/内系统的计划任务可以被列出，默认这些程序以root权限执行，如果某些计划任务执行的脚本或者应用程序对于任意用户可读可写，就可以尝试修改计划任务反弹shell。
- 例如某计划任务要执行的文件是python脚本，而该脚本文件任意用户可读可写，则可以修改该文件的功能为反弹shell到攻击者机器上，然后攻击者机器上面利用nc监听端口，获取shell。

密码复用

- 很多网站管理员都会使用相同的密码，例如网站后台登录密码、数据库登录密码以及服务器系统登录密码可能都是相同的。
- 网站后台登录密码可能会存在的问题就是弱口令和暴力破解，获取到服务器的基础权限以后可以对服务器上面的文件进行读取，通过读取网站中连接数据库的配置文件可以获取数据库用户的登录密码。
- 对于疑似的root用户密码，可以尝试进行ssh远程连接，但是出于安全考虑很多情况下服务器都会禁止root用户远程登录，或者防火墙规则早就将你拒之门外了。
- 同样通过web服务获取到的低权限shell中使用sudo命令不能奏效，也是处于安全性的考虑，Linux要求用户必须从终端设备（tty）中输入密码，而不是标准输入（stdin）。所以需要利用python优化当前获取到的shell，恰巧在Linux操作系统中同样会默认安装python。
  命令：python -c “import pty;pty.spawn(’/bin/bash’)”
- 优化shell以后检测当前用户使用sudo命令的权限
  命令：sudo -l